

**TRANSPORT STREAM PROCESSOR**

**Patent number:** JP2000196586  
**Publication date:** 2000-07-14  
**Inventor:** OKAZAKI WAKAHIKO  
**Applicant:** MATSUSHITA ELECTRIC IND CO LTD  
**Classification:**  
- **international:** H04L9/18; H04L9/14; H04N7/167  
- **european:**  
**Application number:** JP19980370411 19981225  
**Priority number(s):**

**Abstract of JP2000196586**

**PROBLEM TO BE SOLVED:** To provide a transport stream processor where increase in the circuit scale and the required capacity of storage media are suppressed by utilizing device resources so as to conduct efficient processing and a transport stream including encrypted data can properly be processed.  
**SOLUTION:** A PID table register 102 stores correspondence relation among a PID, on/off information and a descramble key number, and a descramble key register 105 stores correspondence relation between the descramble key number and a descramble key. Then a transport packet included in a transport stream is processed on the basis of correspondence relations.



Data supplied from the **esp@cenet** database - Worldwide



## 【特許請求の範囲】

【請求項1】 トランスポートパケットにより構成され、暗号化処理のされたデータを含むトランスポートストリームに対して、上記暗号化処理に対応する復号化処理を行うトランスポートストリーム処理装置において、上記トランスポートパケットに含まれるトランスポートパケットの種別を示すパケット識別情報と、上記復号化処理に関する情報であるパケット復号化情報とを対応させて保持するパケット復号化情報保持手段と、

上記パケット復号化情報と、上記復号化処理に用いられる復号化鍵情報を含む復号化処理情報とを対応させて保持する復号化処理情報保持手段とを備えたことを特徴とするトランスポートストリーム処理装置。

【請求項2】 請求項1に記載のトランスポートストリーム処理装置において、

上記パケット復号化情報保持手段は、上記パケット復号化情報として、復号化処理の要・不要を示す処理制御情報と、上記復号化処理情報の特定に用いられる復号化処理特定情報とを保持するものであり、

上記復号化処理情報保持手段は、上記復号化処理特定情報と、上記復号化鍵情報とを保持するものであることを特徴とするトランスポートストリーム処理装置。

【請求項3】 請求項1に記載のトランスポートストリーム処理装置において、

上記パケット復号化情報保持手段は、上記パケット復号化情報として、上記復号化処理情報の特定に用いられる復号化処理特定情報を保持するものであり、

上記復号化処理情報保持手段は、上記復号化処理特定情報と、上記復号化に用いられる復号化鍵情報、又は復号化処理が不要である旨を示す情報のいずれかである復号化処理情報とを保持するものであることを特徴とするトランスポートストリーム処理装置。

【請求項4】 請求項1に記載のトランスポートストリーム処理装置において、

上記復号化処理情報保持手段は、一の上記復号化処理特定情報と、二以上の上記復号化処理情報とを対応させて保持するものであることを特徴とするトランスポートストリーム処理装置。

## 【発明の詳細な説明】

### 【0001】

【発明の属する技術分野】 本発明はトランスポートストリーム処理装置に関し、特に、トランスポートパケットにより構成され、暗号化処理のされたデータを含むトランスポートストリームに対して、上記暗号化処理に対応する復号化処理を行うトランスポートストリーム処理装置に関する。

### 【0002】

【従来の技術】 データのデジタル化、及び圧縮化技術の進歩に伴い、画像・音声等の記録や、放送を含む伝送に、デジタル画像、デジタル音声の利用が進められてい

る。デジタル化されたデータを記録・伝送に用いることのメリットとしては、画像、音声、文字等を含む各種データを統一的に扱い得るため、サービスの統合化を図り得る点、また、放送ではデータの送受信にあたって圧縮技術を用いることにより、限定された伝送帯域幅を活用して多数の高品質な放送を行い得る点、誤り訂正技術を用いることにより均質なサービスを行い得る点、限定受信のための暗号化技術を容易に利用し得る点など、種々の利点が挙げられる。

【0003】 また、これらデジタル化したデータや、圧縮符号化したデータの送受信にあたっては、データのパケット化が一般的に行われる。パケットとは、データ全体を一定の大きさに分割したデータの単位であり、データをパケットとして送受信することによって、データ通信の効率と精度を上げることが可能となる。例えば、コンピュータネットワークにおいてパケット交換を行う場合では、それぞれのパケットはネットワークを通じて異なったタイミングで各個に転送先に届き、転送先において元のデータに再構成されるので、それぞれのパケットには転送先や発信元、パケットの順番などを知ることのできる情報が付加されている。

【0004】 デジタルデータを扱う場合には、パケット化の技術を用いることにより、映像（静止画情報を含む）、音声（音楽情報を含む）、文字情報、プログラムやサービスに関する情報等の付加情報など各種データをパケット化して組み合わせ、多重化データとし、これを伝送に用いるトランスポートストリーム(transport stream)として記録・伝送することが可能となる。

【0005】 トランスポートストリーム中に含まれるパケットであるトランスポートパケットは、通常、パケット種別等のパケットに関する情報や制御情報を含むヘッダ部と、映像データ、音声データ等のデータを含むデータ部とからなり、ヘッダ部には、パケットの特定に用いられる固有の番号として付与されるPID(パケット識別子: packet identifier)を含むものとなっている。

【0006】 前述のように、デジタル化したデータの取扱いにおいては、暗号化技術の応用が容易であることが大きなメリットの一つとなっている。また、映像・音声等を含む番組を放送するシステム等においては、複数の番組のデータをパケット化し、多重化してトランスポートストリームとして伝送し得るので、複数の番組のうち、特定の番組のみを暗号化して伝送することも可能である。

【0007】 暗号化されたデータを伝送する一般的なシステムでは、送信側においてデータのスクランブル（暗号化）処理を行った上で該暗号化したデータを送信し、受信側においては送信された暗号化データに対して、上記スクランブル処理に対応したデスクランブル（復号化）処理を行うことで、元のデータを得ることとなる。スクランブル（暗号化）は特定のビット系列であるスク

ランブル鍵（暗号化鍵）を用いて、通常のデータを暗号化データに変換することで行われ、これに対応するデスクランブル処理は、スクランブル鍵に対応するデスクランブル鍵（復号化鍵）を用いて、暗号化データを変換して元のデータを取得することでなされることが多い。

【0008】前述のように複数の番組のうち、特定の番組のみ暗号化して伝送する場合など、暗号化されたデータとされていないデータとが混在するトランスポートストリームを処理する場合には、パケット識別子（PID）を用いることで、デスクランブル処理を行うべきパケットを特定することができる。従来の技術による、かかるトランスポートストリームを処理する装置においては、デスクランブル処理を行うべきパケットのPIDと、当該デスクランブル処理に用いるデスクランブル鍵とが処理に先立って設定され、PIDとデスクランブル鍵とを対にして保持し、これに従って処理を行うものである。

【0009】このような、従来の技術によるトランスポートストリーム処理装置に、暗号化されたデータを含むトランスポートストリームが入力されると、当該装置は、入力されたトランスポートストリームを構成するパケットごとにそのパケットのPIDと、デスクランブル処理するべきものとして設定されたPIDとの比較を行う。そして、PIDが一致したならば、そのパケットに対し、設定されたデスクランブル鍵を用いてデスクランブル処理を行う。

【0010】

【発明が解決しようとする課題】従来の技術によるトランスポートストリーム処理装置は、上記のように、デスクランブル処理を行うべきパケットのPIDと、当該デスクランブル処理に用いるデスクランブル鍵とが、予め設定されたものとするすることで、暗号化されたデータとされていないデータとが混在するトランスポートストリームを適切に処理することが可能となる。

【0011】しかし、このような従来の技術による処理装置においては、処理対象となるパケットのPIDと、処理に用いるデスクランブル鍵とを必ず対にして設定しておくものとしているため、PIDの異なるパケットに対して同じデスクランブル鍵を用いて処理を行うことが可能である場合にも、PIDごとに同じデスクランブル鍵を保持しておく必要があり、必ずしも装置資源が活用の点で十分なものでない点が問題となっていた。

【0012】すなわち、PIDの設定数として適切な数と、デスクランブル鍵の設定数として適切な数は同一の値となるとは限らないにもかかわらず、従来の技術による処理装置では、必ず同一の設定値とするような回路構成をとるものとしているため、重複した処理を行う部分が存在するものとなって回路規模が増大しがちであることが問題となっていた。

【0013】又、上記のように、PIDの異なるパケッ

トに対して同じデスクランブル鍵を用いて処理を行うことが可能である場合にも、PIDごとに同じデスクランブル鍵を保持しておく必要があるため、デスクランブル鍵レジスタとして用いる記憶媒体の容量が増大する点、特にデスクランブル鍵は一般的にビット数の大きなデータとなるため、重複したデータを保持するために多量の記憶媒体が用いられ、装置資源が活用されていない点が問題となっていた。

【0014】本発明は、かかる事情に鑑みてなされたものであり、装置資源を活用して効率的な処理を行うことにより、回路規模と記憶媒体の必要量との増大を抑制し、かつ、暗号化されたデータを含むトランスポートストリームを適切に処理することが可能なトランスポートストリーム処理装置を提供することを目的とする。

【0015】

【課題を解決するための手段】上記目的を達成するために、本発明の請求項1にかかるトランスポートストリーム処理装置は、トランスポートパケットにより構成され、暗号化処理のされたデータを含むトランスポートストリームに対して、上記暗号化処理に対応する復号化処理を行うトランスポートストリーム処理装置において、上記トランスポートパケットに含まれるトランスポートパケットの種別を示すパケット識別情報と、上記復号化処理に関する情報であるパケット復号化情報とを対応させて保持するパケット復号化情報保持手段と、上記パケット復号化情報と、上記復号化処理に用いられる復号化鍵情報を含む復号化処理情報とを対応させて保持する復号化処理情報保持手段とを備えたものである。

【0016】また、請求項2にかかるトランスポートストリーム処理装置は、請求項1の装置において、上記パケット復号化情報保持手段は、上記パケット復号化情報として、復号化処理の要・不要を示す処理制御情報と、上記復号化処理情報の特定に用いられる復号化処理特定情報とを保持するものであり、上記復号化処理情報保持手段は、上記復号化処理特定情報と、上記復号化鍵情報とを保持するものである。

【0017】また、請求項3にかかるトランスポートストリーム処理装置は、請求項1の装置において、上記パケット復号化情報保持手段は、上記パケット復号化情報として、上記復号化処理情報の特定に用いられる復号化処理特定情報を保持するものであり、上記復号化処理情報保持手段は、上記復号化処理特定情報と、上記復号化に用いられる復号化鍵情報、又は復号化処理が不要である旨を示す情報のいずれかである復号化処理情報とを保持するものである。

【0018】また、請求項4にかかるトランスポートストリーム処理装置は、請求項1の装置において、上記復号化処理情報保持手段は、一の上記復号化処理特定情報と、二以上の上記復号化処理情報とを対応させて保持するものである。

## 【0019】

【発明の実施の形態】実施の形態1. 本発明の実施の形態1によるトランスポートストリーム処理装置は、パケットの種別を示すPIDと、その種別のパケットに対するデスクランブル処理の要・不要を示す情報と、その種別のパケットに対するデスクランブル処理に用いられるデスクランブル鍵を特定する情報とを対応させて保持するものである。

【0020】図1は、本実施の形態1のトランスポートストリーム処理装置の構成を示すブロック図である。図示するように、本実施の形態1のトランスポートストリーム処理装置100は、トランスポートパケットフィルタ101、PIDテーブルレジスタ102、デスクランブラ103、デスクランブル鍵選択回路104、およびデスクランブル鍵レジスタ105を備えている。

【0021】トランスポートパケットフィルタ101は、入力されるトランスポートストリームに含まれるトランスポートパケットごとに、後述するPIDテーブルレジスタ102に格納されたデスクランブル処理に関する情報を検索して取得し、該取得したデスクランブル処理に関する情報を、後述するデスクランブラ103と、デスクランブル鍵選択回路104とに出力する。また、処理対象となるトランスポートパケットをデスクランブラ103に出力する。

【0022】PIDテーブルレジスタ102は、デスクランブル処理に関する情報であるパケットデスクランブル情報を、PIDと対応させて保持する。パケットデスクランブル情報は、ON/OFF情報と、デスクランブル鍵番号とが組になったものである。あるPIDを有するパケットに対するデスクランブル処理の要・不要は、当該PIDに対応するパケットデスクランブル情報中のON/OFF情報によって知ることができる。又、あるPIDを有するパケットの処理に用いるデスクランブル鍵を取得するためのデスクランブル鍵番号は、当該PIDに対応するパケットデスクランブル情報から取得される。

【0023】すなわち、PIDテーブルレジスタ102は、トランスポートパケットの種別を示すパケット識別情報(PID)と、復号化(デスクランブル)処理の要・不要を示す処理制御情報(ON/OFF情報)、および復号化鍵情報(デスクランブル鍵)の特定に用いられる復号化処理特定情報(デスクランブル鍵番号)からなる、パケット復号化情報(パケットデスクランブル情報)とを対応させて保持するパケット復号化情報保持手段として機能する。

【0024】デスクランブラ103は、トランスポートパケットフィルタ101から入力されたトランスポートパケットに対して、入力された情報に従ってデスクランブル処理を行うか否かを判定し、処理を行う場合は後述するデスクランブル鍵選択回路104から取得するデ

スクランブル鍵を用いてデスクランブル処理を行い、デスクランブル処理済みパケットを生成する。デスクランブル処理済みパケットは当該処理装置の装置出力S160となる。処理を行わない場合には、入力されたトランスポートパケットはデスクランブル処理されることなく、当該処理装置の装置出力S160となる。すなわち、デスクランブラ103は、復号化鍵情報(デスクランブル鍵)を用いて、トランスポートパケットに対する復号化(デスクランブル)処理を行う復号化手段として機能する。

【0025】デスクランブル鍵選択回路104は、トランスポートパケットフィルタ101より入力される情報に基づいて、デスクランブル鍵レジスタ105に格納されたデスクランブル鍵のうちから適切な鍵を選択し、該選択したデスクランブル鍵をデスクランブラ103に出力する。デスクランブル鍵レジスタ105は、デスクランブル鍵を、デスクランブル鍵番号と対にして保持する。すなわち、デスクランブル鍵レジスタ105は、復号化処理特定情報(デスクランブル鍵番号)と、復号化(デスクランブル)処理に用いられる復号化鍵情報(デスクランブル鍵)とを対応させて保持する復号化処理情報保持手段として機能する。

【0026】図2は、本実施の形態1のトランスポートストリーム処理装置100に含まれる、トランスポートパケットフィルタ101、およびPIDテーブルレジスタ102の機能を説明するための、これらの詳細な構成を示すブロック図である。同図において、図1に示すデスクランブラ103、デスクランブル鍵選択回路104、およびデスクランブル鍵レジスタ105については図示を省略する。

【0027】図2において、トランスポートパケットフィルタ101は、PID抽出・選択回路201、PID比較回路202、およびデスクランブル情報選択回路203を備えている。PID抽出・選択回路201は、入力されるトランスポートストリームを構成するトランスポートパケットからPIDを抽出し、抽出したPIDをPID比較回路202に出力する。PID比較回路202は、PID抽出・選択回路201より入力したPID(処理対象PID)を、後述するPIDテーブルレジスタ102において保持されたPIDと比較し、比較の結果一致する場合には、その旨を示す信号を、PID抽出・選択回路201と、デスクランブル情報選択回路203とに出力する。デスクランブル情報選択回路203は、PID選択回路202より一致の旨を示す信号を入力された場合、処理対象PIDに対応するパケットデスクランブル情報を選択し、該選択した情報に含まれるON/OFF情報とデスクランブル鍵番号とを取得する。又、図2に示すPIDテーブルレジスタ102には、複数のPIDとパケットデスクランブル情報との組211～216が格納されている。

【0028】図3は、本実施の形態1のトランスポートストリーム処理装置が処理対象とするトランスポートストリームを説明するための図である。図3(a)は、本実施の形態1の処理装置が用いられる伝送システムにおいて伝送されるトランスポートストリームの構成を示す図である。図示するように、トランスポートストリームは、複数のトランスポートパケットからなり、一つのトランスポートパケットは188バイトの大きさを有するものである。同図(b)は、トランスポートパケットの構成を示す図である。前述のように、パケットはヘッダ部とデータ部とからなるものであり、ここでは4バイトのパケットヘッダがヘッダ部であり、184バイトのアダプテーションフィールド／ペイロードがデータ部である。ヘッダ部はPIDを含んでおり、このPIDは、当該パケットのアダプテーションフィールド／ペイロードが使用されるプログラム(番組)の識別番号を示すものとなっている。また、暗号化されたデータを含むトランスポートパケットでは、ペイロードの部分のみがスクランブル処理されている。

【0029】本実施の形態1の処理装置における、入力されたトランスポートストリームを処理する際の動作について、以下に説明する。図1、および図2に示す構成の本実施の形態1のトランスポートストリーム処理装置は、一般的なMPEGシステム規格に準拠したデジタル放送システムにおいて、図3に示すようなトランスポートストリームを処理するものであって、従来の技術による処理装置と同様に、処理のために必要な情報については、処理に先立って設定しておくものである。

【0030】本実施の形態1の処理装置では、図1に示すPIDレジスタ102において、処理対象となるトランスポートストリームが含むPIDごとに、当該PIDを含むパケットに対するデスクランブル処理の要・不要を示すON/OFF情報が設定され、又、当該PIDを含むパケットのデスクランブル処理に用いるデスクランブル鍵を取得するためのデスクランブル鍵番号が設定される。すなわち、番組ごとに、その番組に含まれるデータのパケットが暗号化(スクランブル処理)されたものであるか否かと、暗号化に対応したデスクランブル処理に必要な鍵を取得するための鍵番号とを設定しておくものである。

【0031】又、デスクランブル鍵レジスタ105には、デスクランブル鍵番号と、デスクランブル鍵との対応関係を示す情報を設定しておくものである。従って、従来の技術による処理装置のように、PIDとデスクランブル鍵との対応関係を保持するものではなく、PIDとデスクランブル鍵番号との対応関係と、デスクランブル鍵番号とデスクランブル鍵との対応関係を保持するものとなる。

【0032】図1に示すように、本実施の形態1の処理装置の装置入力であるトランスポートストリームS15

0は、トランスポートパケットフィルタ101に入力される。トランスポートパケットフィルタ101は、トランスポートストリームS150に含まれるトランスポートパケットごとに以下の処理を行う。トランスポートパケットフィルタ101の動作を図2を用いて説明する。

【0033】まず、トランスポートパケットフィルタ101に含まれるPID抽出・選択回路201は、処理対象とするトランスポートパケットのパケットヘッダに含まれるPIDを抽出し、これをPID比較回路202に出力する。PID比較回路202は、入力された処理対象PIDを、PIDテーブルレジスタ102に格納された、PIDごとのパケットデスクランブル情報との組211~216の各PIDと順次比較し、一致するものを検索する。そして、処理対象PIDが、いずれかのデスクランブル情報との組に含まれるPIDと一致した場合には、PID比較回路202は一致の旨を示す信号をPID抽出・選択回路201と、デスクランブル情報選択回路203とに出力する。

【0034】PID抽出・選択回路201は、PID比較回路202より一致の旨を示す信号を入力された場合、当該トランスポートパケットを、図1に示すデスクランブラ103に出力する。デスクランブル情報選択回路203は、PID比較回路202より一致の旨を示す信号を入力された場合、PIDテーブルレジスタ102より、当該PIDに対応するパケットデスクランブル情報を取得し、該取得したパケットデスクランブル情報中のON/OFF情報とデスクランブル鍵番号とを、図1に示すデスクランブラ103と、デスクランブル鍵選択回路104とにそれぞれ出力する。

【0035】PID比較回路202の処理において、一致するPIDが見いだされ、上記の処理が行われたならば、PID抽出・選択回路201は、トランスポートストリームS150に含まれる次のパケットに対して同様の処理を行う。

【0036】図1において、トランスポートパケットフィルタ101より、デスクランブラ103に対してトランスポートパケットとON/OFF情報とが出力され、デスクランブル鍵選択回路104に対してデスクランブル鍵番号が出力された後の動作を説明する。デスクランブル鍵番号を入力されたデスクランブル鍵選択回路104は、デスクランブル鍵レジスタ105に保持された、デスクランブル鍵番号を検索することによって、当該デスクランブル鍵番号に対応するデスクランブル鍵を取得し、これをデスクランブラ103に出力する。

【0037】デスクランブラ103は、前述のようにトランスポートパケットフィルタ101からデスクランブル処理対象となるトランスポートパケットと、ON/OFF情報とを入力され、又、デスクランブル鍵選択回路104からデスクランブル鍵を入力される。そして、デスクランブラ103は、入力されたON/OFF情報に

従って、トランスポートパケットを処理する。入力されたON/OFF情報がデスクランブル処理不要の旨を示す「OFF」である場合、デスクランブラ103は、トランスポートパケットに対してデスクランブル処理を行うことなくこれを出力する。トランスポートパケットは当該処理装置の装置出力S160となる。

【0038】これに対して、入力されたON/OFF情報がデスクランブル処理要の旨を示す「ON」である場合、デスクランブラ103は、トランスポートパケットに対して、デスクランブル鍵選択回路104から入力されたデスクランブル鍵を用いてデスクランブル処理を行い、デスクランブル処理のなされたデータが当該トランスポートストリーム処理装置の装置出力S160となる。

【0039】このように、本実施の形態1のトランスポートストリーム処理装置によれば、トランスポートパケットフィルタ101、PIDテーブルレジスタ102、デスクランブラ103、デスクランブル鍵選択回路104、およびデスクランブル鍵レジスタ105を備え、PIDテーブルレジスタ102は、PIDとデスクランブル処理の要不要の対応関係と、PIDとデスクランブル鍵番号との対応関係を保持し、デスクランブル鍵レジスタ105は、デスクランブル鍵番号と、デスクランブル鍵との対応関係を保持して、これらの対応関係に基づいて、トランスポートストリームに含まれるトランスポートパケットを適切に処理することが可能となる。

【0040】従って、PIDとデスクランブル鍵との対応関係に基づいて処理を行うため、PIDの設定数とデスクランブル鍵の設定数とが必然的に同一のものとなる従来の技術による処理装置と比較して、双方の設定数を任意のものとできるので、回路の構成において重複処理を行う部分を生じることがなく、回路規模の小型化を図ることが可能となる。

【0041】又、PIDとデスクランブル鍵番号との対応関係において、複数のPIDに対して同一のデスクランブル鍵番号を設定することが可能であり、異なるPIDを有するパケットに対して同一のデスクランブル鍵を用いて処理をすることが可能な場合に、データ量の大きなデスクランブル鍵でなく、データ量の小さなデスクランブル鍵番号を重複設定するので、柔軟に、かつ容易に設定を行い得るものとなり、加えて従来の技術による処理装置と比較して保持のために必要とする記憶媒体の容量を低減することが可能となる。

【0042】実施の形態2. 本発明の実施の形態2によるトランスポートストリーム処理装置は、実施の形態1の処理装置と同様の処理を行うが、処理のための情報の保持状態が異なるものである。図4は、本実施の形態2のトランスポートストリーム処理装置の構成を示すブロック図である。図示するように、本実施の形態2のトランスポートストリーム処理装置400は、トランスポート

パケットフィルタ401、PIDテーブルレジスタ402、デスクランブラ403、デスクランブル鍵選択回路404、およびデスクランブル鍵レジスタ405を備えている。

【0043】このように、本実施の形態2のトランスポートストリーム処理装置の全体構成は、実施の形態1の処理装置と同様のものとなっているが、PIDテーブルレジスタ402と、デスクランブル鍵レジスタ405とにおいて保持する情報が異なるものとなっている。

【0044】PIDテーブルレジスタ402は、実施の形態1の102と同様にデスクランブル処理に関する情報であるパケットデスクランブル情報を保持する。パケットデスクランブル情報は、PIDと、デスクランブル鍵番号とが組になったものであり、実施の形態1の102と異なりON/OFF情報を含まない。特定のPIDを有するパケットの処理に用いるデスクランブル鍵を取得するためのデスクランブル鍵番号がパケットデスクランブル情報から取得される。

【0045】すなわち、PIDテーブルレジスタ402は、トランスポートパケットの種別を示すパケット識別情報(PID)と、復号化処理情報(デスクランブル鍵、またはデスクランブルOFF情報)の特定に用いられる復号化処理特定情報(デスクランブル鍵番号)とを対応させて保持するパケット復号化情報保持手段として機能する。

【0046】デスクランブル鍵レジスタ405は、デスクランブル鍵、又はデスクランブルOFF情報を、デスクランブル鍵番号と対にして保持する。従って、本実施の形態2の処理装置においては、トランスポートパケットに対してのデスクランブル処理の要・不要を示す情報は、デスクランブル鍵レジスタ405が保持する情報より、デスクランブル鍵番号に基づいて得られるものとなる。

【0047】すなわち、デスクランブル鍵レジスタ405は、復号化処理特定情報(デスクランブル鍵番号)と、復号化(デスクランブル)処理に用いられる復号化鍵情報(デスクランブル鍵)、又は復号化処理が不要である旨を示す情報(デスクランブルOFF情報)のいずれかである復号化処理情報とを対応させて保持する復号化処理情報保持手段として機能する。

【0048】図4に示す、トランスポートパケットフィルタ401、デスクランブラ403、およびデスクランブル鍵選択回路404については、入出力する情報の一部が異なることを除いて、実施の形態1(図1)の101、103、および104と同様のものである。また、トランスポートパケットフィルタ401については、図2に示す実施の形態1と同様の内部構成を有するものとすることができる。

【0049】このように構成される本実施の形態2のトランスポートストリーム処理装置に、装置入力であるト

ランスポートストリームS450が入力された場合の、当該装置の動作を以下に説明する。ランスポートストリームS450は、実施の形態1の処理対象であるランスポートストリームS150と同様に、図3に示すようなものであり、パケットヘッダにPIDを含み、一部のランスポートパケットのペイロード部分はスクランブル処理されたものである。

【0050】ランスポートパケットフィルタ401は、処理対象とするランスポートパケットのPIDを抽出し、PIDテーブルレジスタ402が保持する情報を検索して、PIDが一致するパケットデスクランブル情報を取得する。ランスポートパケットフィルタ401は、ランスポートパケットをデスクランブラ403に、PIDテーブルレジスタ402から取得したデスクランブル鍵番号をデスクランブル鍵選択回路404に出力する。

【0051】デスクランブル鍵番号を入力されたデスクランブル鍵選択回路404は、デスクランブル鍵レジスタ405に保持された、デスクランブル鍵番号を検索することによって、当該デスクランブル鍵番号に対応するデスクランブル鍵、またはデスクランブルOFF情報を取得し、これをデスクランブラ103に出力する。

【0052】デスクランブラ403は、デスクランブル鍵選択回路404からデスクランブルOFF情報を入力された場合には、ランスポートパケットに対してデスクランブル処理を行うことなくこれを出力する。ランスポートパケットは当該処理装置の装置出力S460となる。

【0053】一方、デスクランブラ403がデスクランブル鍵選択回路404からデスクランブル鍵を入力された場合には、ランスポートパケットに対して、当該入力されたデスクランブル鍵を用いてデスクランブル処理を行い、デスクランブル処理のなされたデータが当該ランスポートストリーム処理装置の装置出力S460となる。

【0054】このように、本実施の形態2のランスポートストリーム処理装置によれば、ランスポートパケットフィルタ401、PIDテーブルレジスタ402、デスクランブラ403、デスクランブル鍵選択回路404、およびデスクランブル鍵レジスタ405を備え、PIDテーブルレジスタ402は、PIDとデスクランブル鍵番号との対応関係とを保持し、デスクランブル鍵レジスタ405は、デスクランブル鍵番号と、デスクランブル鍵との、またはデスクランブル不要の旨を示す情報との対応関係を保持して、これらの対応関係に基づいて、ランスポートストリームに含まれるランスポートパケットを適切に処理することが可能となる。従って、実施の形態1の処理装置と同様に、回路規模の小型化を図ることが可能となり、処理に先立つ設定が柔軟かつ容易なものであり、デスクランブル鍵保持のために必

要とする記憶媒体の容量を低減することが可能となる。

【0055】実施の形態3. 本発明の実施の形態3によるランスポートストリーム処理装置は、実施の形態2と同様の処理を行うが、デスクランブル鍵、又は処理不要の旨を示す情報の保持の状態が異なるものである。図5は、本実施の形態3のランスポートストリーム処理装置の構成を示すブロック図である。図示するように、本実施の形態3のランスポートストリーム処理装置500は、ランスポートパケットフィルタ501、PIDテーブルレジスタ502、デスクランブラ503、デスクランブル鍵選択回路504、およびデスクランブル鍵レジスタ505を備えている。

【0056】このように、本実施の形態3のランスポートストリーム処理装置の全体構成は、実施の形態2の処理装置と同様のものとなっているが、ランスポートパケットフィルタ501が抽出して、デスクランブル鍵選択回路504に出力する情報の一部と、デスクランブル鍵レジスタ505において保持する情報が異なるものとなっている。

【0057】ランスポートパケットフィルタ501は、実施の形態2と同様の処理に加えて、処理対象とするランスポートパケットより、後述するランスポートスクランブル制御ビットを抽出し、これをデスクランブル鍵選択回路504に出力する。デスクランブル鍵選択回路504は、デスクランブル鍵番号に加えて、このランスポートスクランブル制御ビットをも用いて、デスクランブル鍵レジスタ505において保持されたデスクランブル鍵、又はデスクランブルOFF情報を取得する。

【0058】デスクランブル鍵レジスタ505は、実施の形態2と同様に、デスクランブル鍵、又はデスクランブルOFF情報を、デスクランブル鍵番号と対応させて保持する。実施の形態2では、デスクランブル鍵、又はデスクランブルOFF情報と、デスクランブル鍵番号との対応関係が1対1となるものであったが、本実施の形態3では、2対1の関係となる。図示するように、本実施の形態3のデスクランブル鍵レジスタ505では、一つのデスクランブル鍵番号が、偶数情報、および奇数情報の二つの情報と対応しており、偶数情報、および奇数情報は、それぞれが一つのデスクランブル鍵、またはデスクランブルOFF情報である。

【0059】図6は、本実施の形態3のランスポートストリーム処理装置が処理対象とするランスポートストリームを示す図である。図示するように、このランスポートストリームは、図3に示す実施の形態1、又は2の処理装置の処理対象と同様の形式を有するものであるが、パケットヘッダにランスポートスクランブル制御ビットを含むものである。ランスポートスクランブル制御ビットは、デスクランブル処理に関する情報であり、「偶数」、「奇数」、および「デスクランブルOFF



F」の3つの状態をとるものである。

【0060】図5の構成を有する本実施の形態3のトランスポートストリーム処理装置に装置入力である処理対象トランスポートストリームが入力された場合の、本実施の形態3の装置の動作を以下に説明する。トランスポートパケットフィルタ501は、処理対象とするトランスポートパケットのPIDと、トランスポートスクランブル制御ビットとを抽出する。そして、抽出したPIDに基づいて、PIDテーブルレジスタ502が保持する情報を検索して、PIDが一致するパケットデスクランブル情報を取得する。トランスポートパケットフィルタ501は、トランスポートパケットをデスクランブラ503に、抽出したトランスポートスクランブル制御ビットと、PIDテーブルレジスタ502から取得したデスクランブル鍵番号とをデスクランブル鍵選択回路504に出力する。

【0061】トランスポートスクランブル制御ビットとデスクランブル鍵番号を入力されたデスクランブル鍵選択回路504は、トランスポートスクランブル制御ビットが「デスクランブルOFF」である場合には、デスクランブルOFF情報をデスクランブラ503に出力する。一方、トランスポートスクランブル制御ビットが「偶数」、又は「奇数」である場合には、デスクランブル鍵番号に対応する偶数情報、又は奇数情報を取得してこれをデスクランブラ503に出力する。

【0062】デスクランブラ503は、デスクランブル鍵選択回路504からデスクランブルOFF情報を入力された場合には、トランスポートパケットに対してデスクランブル処理を行うことなくこれを出力する。トランスポートパケットは当該処理装置の装置出力S550となる。

【0063】このように、本実施の形態3のトランスポートストリーム処理装置によれば、トランスポートパケットフィルタ501、PIDテーブルレジスタ502、デスクランブラ503、デスクランブル鍵選択回路504、およびデスクランブル鍵レジスタ505を備え、デスクランブル鍵レジスタ505は、デスクランブル鍵番号と、デスクランブル鍵との、またはデスクランブル不要の旨を示す情報との一対複数の対応関係を保持し、トランスポートパケットに含まれるトランスポートスクランブル制御ビットに基づいて、デスクランブル処理の要・不要を示す情報と、デスクランブル鍵とを取得し、これに基づいて、トランスポートストリームに含まれるトランスポートパケットを適切に処理することが可能となる。従って、実施の形態1の処理装置と同様に、回路規模の小型化を図ることが可能となり、処理に先立つ設定が柔軟かつ容易なものであり、デスクランブル鍵保持のために必要とする記憶媒体の容量を低減することが可能となる。

【0064】

【発明の効果】請求項1のトランスポートストリーム処理装置によれば、トランスポートパケットにより構成され、暗号化処理のされたデータを含むトランスポートストリームに対して、上記暗号化処理に対応する復号化処理を行うトランスポートストリーム処理装置において、上記トランスポートパケットに含まれるトランスポートパケットの種別を示すパケット識別情報と、上記復号化処理に関する情報であるパケット復号化情報とを対応させて保持するパケット復号化情報保持手段と、上記パケット復号化情報と、上記復号化処理に用いられる復号化鍵情報を含む復号化処理情報とを対応させて保持する復号化処理情報保持手段とを備え、パケット識別情報とパケット復号化情報との対応関係、およびパケット復号化情報とパケット復号化処理情報との対応関係に基づいてトランスポートストリームに含まれるトランスポートパケットを適切に処理するので、装置資源の活用によって、回路規模を小型化し、処理に先立つ設定を柔軟かつ容易なものとし、デスクランブル鍵保持のために必要とする記憶媒体の容量を低減することが可能となる。

【0065】請求項2のトランスポートストリーム処理装置によれば、請求項1の装置において、上記パケット復号化情報保持手段は、上記パケット復号化情報として、復号化処理の要・不要を示す処理制御情報と、上記復号化処理情報の特定に用いられる復号化処理特定情報とを保持するものであり、上記復号化処理情報保持手段は、上記復号化鍵特定情報と、上記復号化処理情報とを保持するものとしたことで、保持した対応関係に基づいて、装置資源を活用して適切な処理を行うことが可能となる。

【0066】請求項3のトランスポートストリーム処理装置によれば、請求項1の装置において、上記パケット復号化情報保持手段は、上記パケット復号化情報として、上記復号化処理情報の特定に用いられる復号化処理特定情報を保持するものであり、上記復号化処理情報保持手段は、上記復号化処理特定情報と、上記復号化に用いられる復号化鍵情報、又は復号化処理が不要である旨を示す情報のいずれかである復号化処理情報とを保持するものとしたことで、保持した対応関係に基づいて、装置資源を活用して適切な処理を行うことが可能となる。

【0067】請求項4にかかるトランスポートストリーム処理装置によれば、請求項1の装置において、上記復号化処理情報保持手段は、一の上記復号化処理特定情報と、二以上の上記復号化処理情報とを対応させて保持するものとしたことで、保持した対応関係に基づいて、装置資源を活用して適切な処理を行うことが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態1によるトランスポートストリーム処理装置の構成を示すブロック図である。

【図2】同実施の形態の装置の、一部の詳細な構成を示すブロック図である。

【図3】同実施の形態の装置が処理対象とするトランスポートストリームを示す図である。

【図4】本発明の実施の形態2によるトランスポートストリーム処理装置の構成を示すブロック図である。

【図5】本発明の実施の形態3によるトランスポートストリーム処理装置の構成を示すブロック図である。

【図6】同実施の形態の装置が処理対象とするトランスポートストリームを示す図である。

【符号の説明】

101, 401, 501 トランスポートパケットフ

イルタ

102, 402, 502 PIDテーブルレジスタ

103, 403, 503 デスクランブラ

104, 404, 504 デスクランブル鍵選択回路

105, 405, 505 デスクランブル鍵レジスタ

201 PID抽出・選択回路

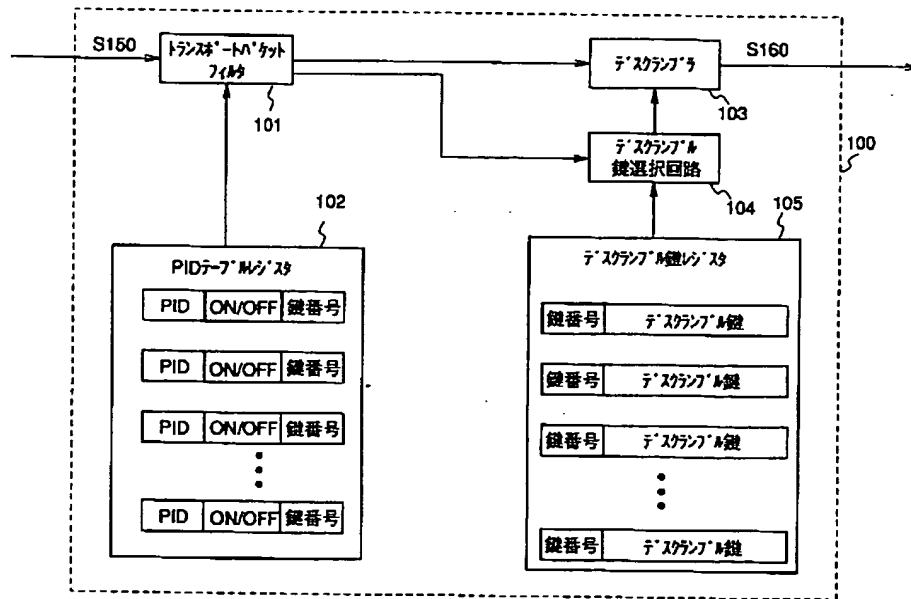
202 PID比較回路

203 デスクランブル情報選択回路

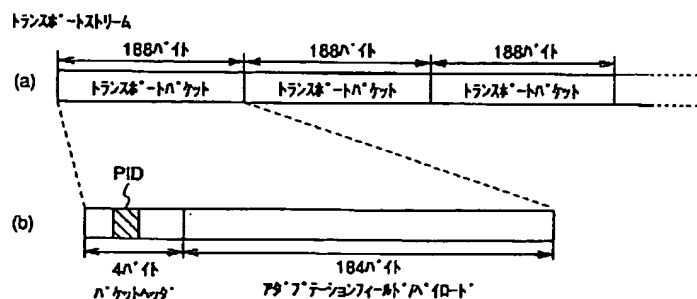
211, 212, 213, 214, 215, 216

PID、パケットデスクランブル情報組

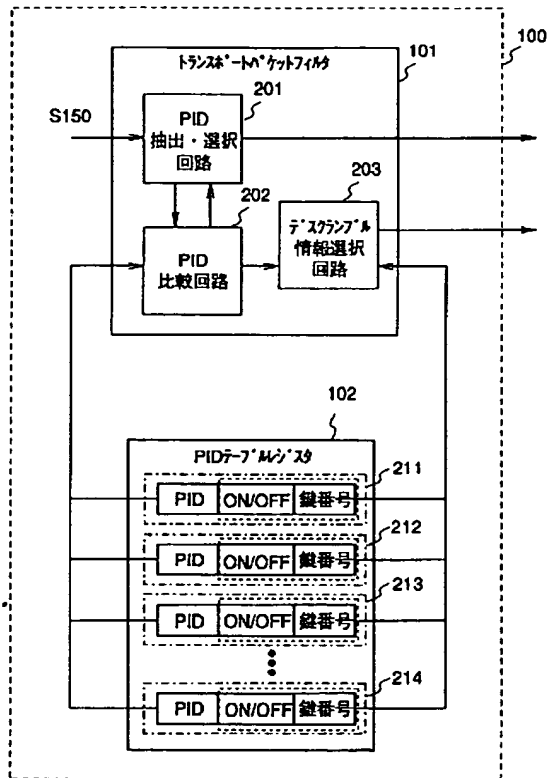
【図1】



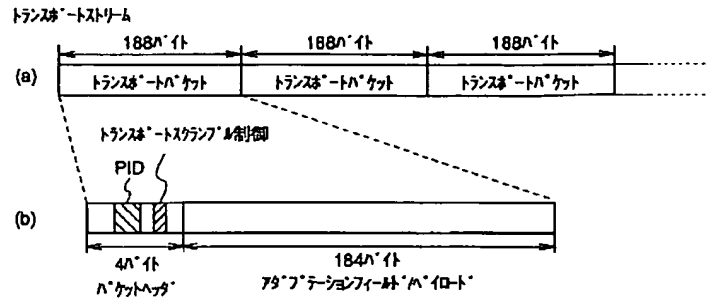
【図3】



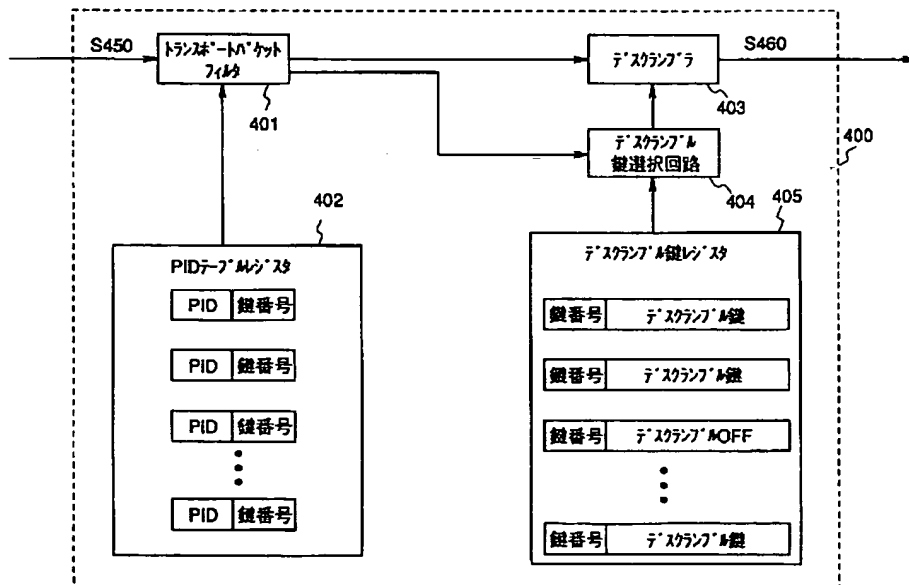
【図2】



【図6】



【図4】



【図5】

